"APPROVED"
by Order No. ___
dated "___" _____ 2025
of the General Director of Amana Virtual Assets Exchange LLC

Amana Virtual Assets Exchange Limited Liability Company

Rules Aimed at Ensuring Compliance with the Requirements of the Legislation on Counteracting the Legalization (Laundering) of Proceeds Derived from Criminal Activity and the Financing of Terrorism

1. **GENERAL PROVISIONS**

1.1. These Rules have been developed in accordance with the Law of the Kyrgyz Republic “On Counteracting the Financing of Terrorist Activity and the Legalization (Laundering) of Criminal Proceeds” (hereinafter – the Law on CFT/AML), as well as other regulatory legal acts of the Kyrgyz Republic.
1.2. The purpose of these Rules is to establish the minimum requirements for the organization of internal control within the Organization for the purposes of CFT/AML, as well as for the execution of transactions exhibiting characteristics of suspicious transactions.
1.3. Amana Virtual Assets Exchange LLC (hereinafter – the Company) strictly complies with the legislation of the Kyrgyz Republic in the field of counteracting the financing of terrorist activity and the legalization (laundering) of criminal proceeds (CFT/AML).

2. COMPANY ACTIVITIES IN THE FIELD OF COUNTERACTING THE FINANCING OF TERRORIST ACTIVITY AND THE LEGALIZATION (LAUNDERING) OF CRIMINAL PROCEEDS

2.1. During client onboarding and servicing, the Company strictly adheres to Know Your Customer requirements, which entail the collection and verification of comprehensive data necessary for proper identification of the client. The client shall provide full name, date of birth, citizenship, and an identity document (passport or other official document indicating the number, series, date of issue, and containing a photographic image), supplemented by a current residential address and contact details. In addition, information regarding the client's occupation and the sources of funds shall be requested. These measures comply with international standards, including the recommendations of the Financial Action Task Force, as well as the requirements of national legislation, including the Law of the Kyrgyz Republic dated 6 August 2018 No. 87 "On Counteracting the Legalization (Laundering) of Criminal Proceeds and the Financing of Terrorism."

2.2. The Company applies these Rules to discharge the following principal obligations:

1) implementation of measures for the identification, assessment, monitoring, management, mitigation, and documentation of risks;
2) implementation of customer due diligence measures;
3) application of targeted financial sanctions and suspension of transactions;
4) implementation of measures with respect to high-risk countries;
5) timely submission to the financial intelligence authority of information, documents, and reports on transactions subject to control and reporting.;

3. KNOW YOUR CUSTOMER PROCEDURES AND RISK ASSESSMENT

3.1. During client onboarding and servicing, the Company strictly adheres to Know Your Customer requirements, which entail the collection and verification of comprehensive data necessary for proper identification of the client. The client shall provide full name, date of birth, citizenship, and an identity document (passport or other official document indicating the number, series, date of issue, and containing a photographic image), supplemented by a current residential address and contact details. In addition, information regarding the client's occupation and the sources of funds shall be requested. These measures comply with international standards, including the recommendations of the Financial Action Task Force, as well as the requirements of national legislation, including the Law of the Kyrgyz Republic dated 6 August 2018 No. 87 "On Counteracting the Legalization (Laundering) of Criminal Proceeds and the Financing of Terrorism."

3.2. The Company verifies the authenticity of the documents and information provided. Advanced identity verification methods shall be applied, including verification of passport data through state databases where available, as well as biometric identification. The Company shall not grant access to its services until the client's identity has been successfully verified within the framework of the Customer Identification Program.

3.3. Upon completion of the Know Your Customer procedures, the Company conducts a risk assessment with respect to each client and assigns the client to an appropriate risk category (low, medium, high). The assessment criteria include, inter alia, the results of screening against sanctions lists and watchlists, the client's status, the country of residence and business registration, the intended purpose of using the virtual asset services, and the anticipated transaction volumes. Based on these factors, the client's risk profile shall be established. Clients classified as presenting elevated risk shall be subject to enhanced due diligence measures. Within the framework of enhanced due diligence, additional documents and information may be requested, including proof of address, financial statements, and information regarding beneficial owners. The provision of services to such clients shall be subject to approval by the Company's management. This risk-based methodology is consistent with internationally recognized best practices and enables the application of proportionate control measures tailored to each client.

3.4. **Handling of Politically Exposed Persons**

1) The Company assigns heightened importance to the identification of politically exposed persons among its clients. Within the framework of the Know Your Customer procedures, each client shall indicate in the relevant questionnaire whether the client or any close family members or associated persons qualify as politically exposed persons, including, inter alia, individuals holding public office. In addition to client self-declaration, the Company independently conducts screening using specialized databases of politically exposed persons containing information on political figures, public officials, and their relatives. This dual approach ensures the reliability of identification, as the system may detect politically exposed person status through external sources even where such status has not been disclosed by the client. Where politically exposed person status is identified, such information shall be recorded in the client's profile, and the client shall be assigned a high-risk classification.
2) Clients classified as politically exposed persons shall be automatically subject to enhanced verification procedures. The Company conducts comprehensive due diligence procedures with respect to politically exposed persons. Within the framework of enhanced due diligence, additional information and documentation shall be requested to confirm the client's integrity and the lawful origin of funds. By way of example, the Company may require the submission of income declarations, bank statements, or other financial documentation demonstrating that the client's financial position is commensurate with the anticipated transactions. References from servicing banks or other financial institutions may also be requested. The purpose of these measures is to ensure that the funds of politically exposed persons are not associated with corruption, bribery, or other abuses of public office. All collected documentation shall be reviewed by the compliance function, and any decision to establish or continue the business relationship shall be subject to approval by the Company's management.
3) Transactions and accounts associated with politically exposed persons shall be subject to enhanced monitoring and control. Reduced thresholds for the identification of transactions as large or unusual shall

be applied. Any transaction conducted by a politically exposed person, or through an account beneficially owned or controlled by a politically exposed person, shall be assessed for consistency with the client's risk profile. Transaction amounts shall be evaluated against the known sources of income, and the purpose of payments shall be subject to scrutiny. The Company applies the principle of dual control to transactions involving politically exposed persons, whereby significant or atypical transactions are subject to both automated monitoring mechanisms and manual review by a compliance officer. Where a transaction gives rise to concerns, the client may be requested to provide clarifications and supporting documentation. In cases of serious suspicion, the transaction may be suspended and the applicable internal reporting procedures initiated.

4) The establishment of a business relationship with a politically exposed person, or the continuation of servicing of such a client, requires approval by the Company's senior management. Information concerning the presence of politically exposed persons among the Company's clients shall be reflected in internal compliance records and communicated to the Head of Compliance and the Company's management. The status of politically exposed persons shall be reviewed on a periodic basis. All information relating to politically exposed persons shall be handled with an enhanced level of confidentiality. Upon receipt of lawful requests from competent regulatory authorities or the financial intelligence authority concerning transactions involving politically exposed persons, the Company shall provide all requested information and documentation in accordance with applicable legal requirements.

3.6 **Identification of Ultimate Beneficial Owners**

1) In accordance with international standards and the legislation of the Kyrgyz Republic, the Company shall mandatorily establish the identity of ultimate beneficial owners of its clients that are legal entities. An ultimate beneficial owner shall be understood as a natural person who ultimately owns or controls, directly or indirectly, more than twenty-five percent of the ownership interests in the client or otherwise exercises control over the client's activities. The ultimate beneficial owner identification procedure is intended to prevent the use of nominee arrangements designed to conceal the identity of the true beneficiaries.
2) Upon the establishment of a business relationship, the client shall disclose the ownership and control structure of the legal entity up to the level of the ultimate natural persons. For the purposes of verification, the Company shall request identification documents and information equivalent to those required for natural persons, including identity documents and proof of address, as well as documentation evidencing ownership interests. Where the ownership structure is complex or multi-layered, the client shall provide documentary evidence substantiating each level of the ownership chain. Where the ultimate beneficial owner cannot be identified, or where doubts arise as to the accuracy or completeness of the information provided, the ultimate beneficial owner shall be deemed to be the natural person exercising senior executive control over the client.
3) Information relating to ultimate beneficial owners shall be subject to thorough verification. All identified ultimate beneficial owners shall be screened against applicable sanctions lists, lists of persons associated with terrorist or extremist activities, and databases of politically exposed persons. Where an ultimate beneficial owner is identified as a politically exposed person or as a resident of a high-risk jurisdiction, the client legal entity shall be automatically subject to enhanced due diligence measures.

3.7 Sanctions Lists and Screening

1) The Company strictly complies with applicable sanctions regimes and conducts screening of clients

against international sanctions lists. Within the Know Your Customer onboarding process, each new client shall be subject to screening against up-to-date sanctions lists. National sanctions lists shall also be taken into account where required by competent regulatory authorities. To ensure the effectiveness and accuracy of such controls, the Company employs specialized automated systems designed to compare the client's identifying data, including full name, date of birth, and citizenship, with the records contained in the relevant sanctions databases. This process enables the Company, at the client acceptance stage, to confirm the absence of any sanctions designation or affiliation with sanctioned persons or entities.

2) Sanctions compliance shall be maintained on a continuous basis. The Company's client database shall be regularly screened against updates to applicable sanctions lists no less frequently than once per day. Where an existing client becomes subject to sanctions during the course of the business relationship, the monitoring systems shall generate an immediate alert. In such circumstances, the Company shall promptly implement all necessary restrictive measures, including the suspension of transactions, the blocking of withdrawal capabilities, and the initiation of an internal review. The identification of a sanctioned person among the Company's clients shall be communicated to the competent regulatory authorities as required by law. Any subsequent actions shall be undertaken in strict accordance with applicable legal and regulatory requirements.

4. TRANSACTION MONITORING AND DETECTION OF SUSPICIOUS ACTIVITY

4.1. The Company performs monitoring of all client transactions. For these purposes, the Company utilizes a specialized anti-money laundering platform designed to analyze blockchain transactions against established risk criteria. The system continuously tracks the movement of virtual assets across wallets associated with the platform and evaluates transactions by reference to known typologies and relevant databases. Monitoring measures extend to all principal virtual assets supported by the platform, including tokens issued under the ERC-20 standard and other digital assets.

4.2. The monitoring system evaluates each transaction using a range of risk indicators. Such indicators include, inter alia, the transaction amount, the frequency and sequence of transactions, related wallet addresses, and relevant geographic factors. Transactions that materially deviate from the client's established transaction profile, including unusually large amounts, atypical transaction flows, or the structuring of transfers into multiple smaller transactions, shall be treated as potentially suspicious. Particular attention shall be given to transactions involving anonymization services or transactions connected to high-risk jurisdictions. The system assigns a risk rating to each transaction or wallet address based on historical data, behavioral analysis, and known associations, including potential links to illicit activities or previously identified unlawful schemes. Where a transaction exceeds predefined risk thresholds or meets multiple risk criteria, it shall be flagged for further review. As a result of such automated analysis, the system generates a set of triggers indicative of suspicious transactions.

4.3. The transaction monitoring technology is integrated with sanctions databases and databases of prohibited or high-risk subjects. All transactions shall be assessed for the involvement of sanctioned persons or entities. The system automatically compares wallet addresses involved in transactions with addresses included in international sanctions lists, including those maintained by the United Nations, the Office of Foreign Assets Control, the European Union, and other competent authorities. Where a match is identified, the transaction shall be immediately classified as suspicious. Similarly, transactions involving addresses previously identified as associated with terrorist organizations or other prohibited entities shall be assigned a high-risk classification.

4.4. All transactions flagged by the monitoring system as suspicious shall be subject to enhanced review by the compliance function. The responsible specialists shall analyze the transaction details, assess their consistency with the client's risk profile, and evaluate all other relevant information available to the Company. Where necessary, additional information and supporting documentation may be requested from the client, including explanations of the economic rationale of the transaction and documents evidencing the lawful origin of funds. During the course of such review, the transaction may be suspended or temporarily restricted at the platform level until all relevant circumstances have been duly clarified. Where the review determines that the initial concerns are not substantiated, the transaction shall be released and processed in the ordinary course. Where the review results in the confirmation or escalation of suspicion, the Company shall initiate the applicable internal reporting procedures, including the preparation of a Suspicious Activity Report. This multi-layered control framework, combining automated detection mechanisms with manual compliance review, ensures a robust system of anti-money laundering oversight.

5. RETENTION OF INFORMATION AND DOCUMENTATION

5.1 The Company assigns particular importance to the secure retention and protection of information collected within the framework of Know Your Customer procedures and transaction monitoring activities. All client-related information, including identification documents, questionnaires, addresses, and records of communications, as well as transaction data, shall be maintained within secure information systems. Access to such systems shall be strictly limited to duly authorized personnel of the compliance and security functions. The Company utilizes technological infrastructure designed to meet applicable information security and cybersecurity requirements, including the application of data encryption measures. In accordance with the requirements of the legislation of the Kyrgyz Republic, client identification data and transaction records shall be retained for a minimum period of five years following the termination of the business relationship, or for such longer period as may be required by applicable legal or regulatory provisions. Such retention requirements ensure the availability of information for retrospective analysis and for submission to competent authorities upon lawful request. Records of transactions and Suspicious Activity Reports shall be retained for the legally prescribed retention period. The Company processes and retains personal data on the basis of valid client consent and in compliance with the legislation governing personal data protection. Internal policies require the implementation of periodic data backup procedures and the application of measures designed to prevent unauthorized access, disclosure, or data leakage. Client information shall be stored and processed primarily within the territory of the Kyrgyz Republic in accordance with applicable data localization requirements. These measures collectively ensure compliance with regulatory obligations and the safeguarding of client confidentiality.

6. COOPERATION WITH STATE AUTHORITIES AND REPORTING OF SUSPICIOUS ACTIVITY

6.1 Upon the identification of a transaction or activity giving rise to suspicion as to the legality of the source of funds or the purpose of the transaction, the Company shall prepare a special report, namely a Suspicious Activity Report. The designated employee responsible for financial monitoring shall record in the report all relevant details pertaining to the matter, including client identification data, a description of the activity, the grounds upon which such activity has been classified as suspicious, with reference to specific criteria or indicators, as well as any internal measures undertaken, including, inter alia, the suspension of the transaction where applicable. The report shall be subject to internal approval by the Head of Compliance and, where necessary, the legal function, following which it shall be submitted to the competent state authority, namely the Financial Intelligence Service under the Ministry of Finance of the Kyrgyz Republic.

6.2 In accordance with the requirements of the legislation of the Kyrgyz Republic, information relating to suspicious activity shall be submitted in a timely manner to the competent authorities responsible for financial monitoring. The Company shall submit the prepared Suspicious Activity Report to the Financial Intelligence Service of the Kyrgyz Republic, acting as the financial intelligence unit of the Kyrgyz Republic. Simultaneously, where required, the Company shall notify the competent supervisory authority responsible for the regulation and oversight of virtual asset service providers. Reports concerning suspicious transactions shall be submitted without delay following their

preparation and within the timeframes established by applicable legislation.

6.3 In addition to the submission of individual reports concerning suspicious transactions, the Company shall comply with its obligations concerning periodic regulatory reporting. The Company shall prepare and submit all reports required under applicable legislation, including, inter alia, reports on the implementation of internal anti-money laundering controls, the number of Know Your Customer procedures conducted, and statistical data concerning identified suspicious activities. Such reports shall be submitted to the competent supervisory authorities in accordance with the prescribed reporting schedules. Upon receipt of lawful requests from competent state authorities, the Company shall provide ad hoc reports, explanations, or supporting documentation. The Company shall maintain a complete record of all Suspicious Activity Reports submitted and of all measures undertaken in connection with such cases. The Company shall ensure prompt cooperation with competent authorities, including law enforcement bodies and the financial intelligence authority, and shall provide all requested information within the scope of its legal obligations. All employees involved in reporting processes shall ensure the confidentiality of transmitted information and full compliance with personal data protection requirements.

6.4 The Company shall designate an officer responsible for compliance with anti-money laundering and counter-terrorist financing requirements. The designated officer shall ensure the effective implementation and ongoing operation of the anti-money laundering program within the Company and shall serve as the primary point of contact for interaction with competent state authorities. The Company shall cooperate fully with supervisory and regulatory authorities and shall be prepared for scheduled and unscheduled inspections. The Company shall provide competent authorities with access to all documentation, records, and reports required for the performance of supervisory functions. The Company shall conduct periodic internal audits and assessments of the effectiveness of its anti-money laundering controls. Where deficiencies or violations are identified, the Company shall promptly implement corrective measures and, where required by law, notify the competent authorities. This approach ensures regulatory transparency and compliance with applicable legal obligations.

6.5 Taking into account the specific regulatory framework applicable to virtual asset activities in the Kyrgyz Republic, the Company shall comply with all additional regulatory requirements imposed upon virtual asset service providers. In particular, the Company shall implement the Travel Rule in accordance with applicable legal and regulatory provisions and internationally recognized standards. In respect of virtual asset transactions exceeding the legally established threshold, the Company shall collect, retain, and transmit the required identifying information relating to the originator and the beneficiary of the transfer. Such information shall include, inter alia, the name of the originator, the relevant account or wallet identifiers, beneficiary information, and transaction identifiers. The Company shall also comply with mandatory financial monitoring thresholds, including the reporting of transactions exceeding prescribed limits, irrespective of whether such transactions have been classified as suspicious. The Company shall observe all applicable tax, regulatory, and reporting obligations arising under the legislation of the Kyrgyz Republic. Compliance with the foregoing requirements shall constitute an integral component of the Company’s operations and shall be subject to oversight at the management level.

7. FINAL PROVISIONS

7.1. These Rules shall be subject to amendment in the event of changes to the legislation of the Kyrgyz Republic.
7.2. Matters not governed by these Rules shall be regulated by the applicable legislation of the Kyrgyz Republic, internationally recognized practices, and the internal documents of the Company.
7.3. In the event that, as a result of amendments to the legislation or regulatory legal acts of the Kyrgyz Republic, certain provisions of these Rules conflict with such amendments, the relevant provisions shall become invalid to the extent of such conflict and shall remain inapplicable until the corresponding amendments to these Rules are duly adopted.
7.4. These Rules shall enter into force as of the date of their approval by the Director of the Company.